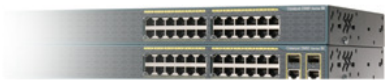
Login About Cisco

ASA Phone Proxy sample configuration - Ciscowiki

HelpFeedback

- Article
- Discussion
- View source
- History



ASA Phone Proxy sample configuration

From Ciscowiki

Contents

Overview

The Cisco ASA phone proxy feature allows remote Cisco IP phones to establish secured communication channels directly with the ASA. These secure communications terminate directly onto the firewall, and the firewall "proxies" the voice communication between the phone and the Call Manager.

This feature allows for secure voice communication for phones deployed in the field without requiring a separate device to encrypt the traffic to the Call Manager.

To configure ASA Phone Proxy via ASDM, please reference this page: http://supportwiki.cisco.com/wiki/index.php/ASA_Phone_Proxy_sample_configuration_via_ASDM

Terminology

Media Termination Address

The Media Termination Address is an address that the firewall uses to perform the phone proxy function. It is a special address that is used to terminate secure media streams to and from remote phones. This address needs to be a unique, publicly routeable address on the outside of the firewall, and must adhere to the following guidelines:

- It must not be the same as any global address for any translation on the firewall
- It must be a different address than the outside interface address of the firewall (or any other firewall interface)
- It must reside in the same ip subnet as the outside interface of the firewall
- No other device on the outside subnet can also be assigned this IP address

SRTP

SRTP (Secured Real-time Transport Protocol) refers to RTP (Real-time Transport Protocol) media streams which are encrypted.

Certificate Trust List (CTL) File

The CTL file is a file that the phone downloads when it first connects to the tftp server upon bootup. The CTL file contains information about what devices the phone can trust, along with the certificates for those devices. In the case of phone proxy the firewall is configured to generate and send its own CTL file to the remote phone. The CTL file contains the certificates for the devices in the phone proxy environment, such as the Call Manager(s), tftp-server and CAPF certificates.

MIC and LSC Certificates

There are two types of certificates that can be present on Cisco IP Phones:

- Manufacturer Installed Certificate (MIC)
- Locally Significant Certificate (LSC)

For the phone proxy feature to function propery and for the traffic between the phone and the ASA to be encrypted, the phone must have a certificate installed. To determine if a phone has a certificate already installed on the phone, press the Settings button, then choose "6 - Security Configuration" then scroll down and look for the sections labelled "MIC" and "LSC". If either of these reads "Installed" a certificate of that type is installed. If it reads "Not Installed" there is no certificate of that type installed.

CAPF

Stands for Certificate Authority Proxy Function. This is a feature that runs on the Cisco Unified Call Manager Publisher that can deploy LSC certificates to phones. This is required for phones that do not have a MIC certificate to establish secure or authenticated connections. More information on the process of deploying certificates to phones using the CAPF process can be found at the documentation link below

Call Manager 7.0 CAPF docs

It is important that phone proxy deployments not use MIC certificates except for initial setup, as any cisco phone with a MIC will be able to connect to the phone proxy if the MIC certificates are installed. It is advisable to use the MIC certificates to deploy LSC certificates, so that only authorized phones (with the correct certificate) can connect to the phone proxy.

Prerequisites

The following are required before the phone proxy feature will work correctly

Search

- The remote Cisco IP phone must have a certificate installed for the secure connection to be made to the firewall
- The ASA firewall must be running at least version 8.0(4)
- The ASA must have the appropriate license installed. To determine the number of secured connections available, use the "show version" command. Each phone to Call Manager connection counts as one secure connection; Therefore, if two Call Managers are present (and in a redundant configuration) since each phone maintains two connections (one to each Call Manager) then a total of two licenses will be used for each phone.

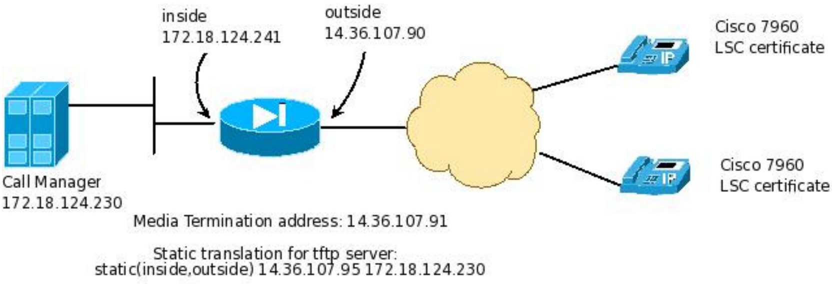
Note the line that reads "UC Proxy Sessions":

```
PhoneProxyASA#show version

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 5.2(4)
....
UC Proxy Sessions            : 2
```

Step-by-Step configuration example

For this example, the following diagram depicts the network:


inside
172.18.124.241
outside
14.36.107.90
Cisco 7960
LSC certificate
Cisco 7960
LSC certificate
Call Manager
172.18.124.230
Media Termination address: 14.36.107.91
Static translation for tftp server:
static(inside,outside) 14.36.107.95 172.18.124.230

- The outside interface is meant to represent the internet in this example.
- The media termination address is 14.36.107.91.
- The TFTP server resides on the call manager, and the call manager is at 172.18.124.230. The firewall is statically translating this inside ip to the outside with a global address of 14.36.107.95.
- The phones in this case have a LSC certificate installed using the CAPF process. This certificate was previously installed on the phone by the Call Manager prior to introducing it to the phone-proxy
- The Call Manager is running in non-secure mode. Therefore all communication from the ASA to the call manager will be unencrypted

The following configuration is based off of the configuration guide located here

1. Set the hostname and domain-name of the firewall. These settings will be used when the RSA keys are generated in step 4.

```
ciscoasa# conf t
ciscoasa(config)# hostname PhoneProxyASA
PhoneProxyASA(config)# domain-name cisco.com
PhoneProxyASA(config)#
```

2. (Optional) Configure DNS resolution on the ASA if the Call Manager server is configured by hostname, rather than IP address. If the Call Manager is configured by hostname then it will insert its own hostname into the TFTP config file sent to the phone, instead of its IP address; the phone will then attempt to resolve the hostname and connect to the resulting ip. The phone, as well as the ASA, will need to be able to resolve the IP of the Call Manager if this is the case. You can check to see if the Call Manager server is configured by hostname by going to the Call Manager and under "System->Server" and press the "Find" button to display the Call Manager description. It will show an IP address or a Hostname. If your Call Manager is configured by ip address, this step is not necessary, as the phone and the ASA won't need to do any dns resolution.

In the following example:

- The DNS server resides on the outside
- The DNS server ip address is 172.18.108.43
- In this case the DNS server is added to the default DNS server group

```
PhoneProxyASA(config)# dns domain-lookup outside
PhoneProxyASA(config)# dns server-group DefaultDNS
PhoneProxyASA(config-dns-server-group)#     name-server 172.18.108.43
```

3. Create a static translation so that the Call Manager's TFTP server is accessible from the outside internet. The phones will be configured with the 14.36.107.95 address as their TFTP server:

```
PhoneProxyASA(config)# static (inside,outside) 14.36.107.95 172.18.124.230 netmask 255.255.255.255
```

4. A keypair needs to be generated that will be used for the self-signed certificate on the firewall. If a keypair is already created then this step can be skipped.

```
PhoneProxyASA(config)# crypto key generate rsa label proxy_key modulus 1024
INFO: The name for the keys will be: proxy_key
Keypair generation process begin. Please wait...
PhoneProxyASA(config)#
```

5. Next, create a trustpoint that will be used for secure communication with the remote phones. In this case we'll call this trustpoint phoneproxy_trustpoint. After creating the trustpoint, we enroll the trustpoint immediately (causing the firewall to generate the self-signed certificate).

Go Search

```
PhoneProxyASA(config)# crypto ca trustpoint phoneproxy_trustpoint
PhoneProxyASA(config-ca-trustpoint)# enrollment self
PhoneProxyASA(config-ca-trustpoint)# keypair proxy_key
PhoneProxyASA(config-ca-trustpoint)# exit
PhoneProxyASA(config)#
PhoneProxyASA(config)# crypto ca enroll phoneproxy_trustpoint
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: PhoneProxyASA.cisco.com

% Include the device serial number in the subject name? [yes/no]: no

Generate Self-Signed Certificate? [yes/no]: yes
PhoneProxyASA(config)#
```

6. (Optional - Only necessary if the phones have a LSC installed and no MIC) If the phones we are using do not have a MIC certificate (and the only certificate that they have is a LSC) then we'll need to add the CA CAPF certificate from the Call Manager. Again, this step is only necessary if the remote phones have a LSC certificate loaded.

To retrieve the CAPF certificate from the Call Manager running version 5.1, do the following (these steps might be different depending on the Call Manager version):

1. Log into the Call Manager web interface
2. In the upper right of the screen in the "Navigation" selector, choose "Cisco Unified OS Administration" and click "Go"
3. Choose the "Security" drop down, then choose "Certificate Management" then "Download Certificate / CTL"
4. Choose "Download Trust Cert" and then "CAPF". Download this certificate in .pem encoding.

Then, create the trustpoint and import the CAPF CA certificate from the Call Manager onto the firewall

```
PhoneProxyASA(config)# crypto ca trustpoint capf_trustpoint
PhoneProxyASA(config-ca-trustpoint)# enrollment terminal
PhoneProxyASA(config-ca-trustpoint)# exit
PhoneProxyASA(config)# crypto ca authenticate capf_trustpoint
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIICdDCCAd2gAwIBAgIIFgGX+wPCb6YwDQYJKoZIhvcNAQEFBQAwVTEKMAgGA1UE
ChMBQTEKMAgGA1UECBMBRDEKMAgGA1UEBxMBQzELMAkGA1UEBhMCVVMxFjAUBgNV
BAMTDUNBUEYtMTViYjNkZjgxCjAIBgNVBAsTAUIwHhcNMDcwOTA0MTEwODM0WhcN
MTIwOTA0MTEwODM0WjBVMQowCAYDVQQKEwFBMQowCAYDVQQIEwFEMQowCAYDVQQH
EwFDMQswCQYDVQQGEwJVUzEWMBQGA1UEAxMNQ0FQRi0xNWJiM2RmODEKMAgGA1UE
CxMBQjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAujDQz2fuaz/lorFoVFPF
KWYLfYzq8CuBvBl18pfHvdFbmtZcWkm3wY/s+9HCxh6FqzjXKpQM8sQQ6TfA80Gf
qNKTqypDJnRhMv/+C7eh4XuV4hFMl82MFaZvcmVTtjkpdrcv5iRZn1OCOg3JEaLS
CAONhglqQgKQqrxOHqxpoZ0CAwEAAaNNMEswCwYDVR0PBAQDAgKEMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDBTAdBgNVHQ4EFgQU9S/3lbgkdbAMDeTnhAXC
xEUAkcswDQYJKoZIhvcNAQEFBQADgYEAhTlglsQnxcwMxMtWM8uZIg6ya8dt3zP4
RBuKqD2PZWH5d/fe9rGvf/TZqSGhGjxa1N6e0kRS29UUy/4u2zr7iGqpZXyezrfc
3+/q8z6YvBx6qH+BSG4KKnC9iQ+2YbMBXn93HlQK+kwJGXEngOkJY45pIaNn6dOA
bp9pXH9Si24=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     1f53d57a 5d82b8e7 4f7f9ceb 1758e181
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
PhoneProxyASA(config)#
```

7. It is necessary to load the Cisco Manufacturer CA certificates onto the firewall so that phones that use MIC certificates and the firewall can make a secure connection. Therefore, we'll create a trustpoint for each of the CA certificates CAP-RTP-001, CAP-RTP-002, and Cisco_Manufacturing_CA. These CA certificates can be downloaded from the Call Manager by doing the following (these steps might be different depending on the Call Manager version):

1. Log into the Call Manager web interface
2. In the upper right of the screen in the "Navigation" selector, choose "Cisco Unified OS Administration" and click "Go"
3. Choose the "Security" drop down, then choose "Certificate Management" then "Download Certificate / CTL"
4. Choose "Download Trust Cert" and then "Call Manager - Trust". Download the certificates (CAP-RTP-001, CAP-RTP-002, and Cisco_Manufacturing_CA) in .pem encoding.

Now, create a trustpoint for each certificate and authenticate them all with the downloaded .pem encoded files:
Personal tools

- This page was last modified 19:42, 13 November 2008.

```
PhoneProxyASA(config)#  crypto ca trustpoint CAP-RTP-001_trustpoint
PhoneProxyASA(config-ca-trustpoint)# enrollment terminal
PhoneProxyASA(config-ca-trustpoint)# exit
PhoneProxyASA(config)# crypto ca authenticate CAP-RTP-001_trustpoint
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzM2MzRaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAxMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEArFW77Rjem4cJ/7yPLVCauDohwZZ/3qf0sJaWlLeAzBlq
Rj2lFlSij0ddkDtfEEo9VKmBOJsvx6xJlWJiuBwUMDhTRbsuJz+npkaGBXPOXJmN
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6Rexgscfz6ypG270qSac
cK4FoJowbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAxL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDEuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMVxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAxLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAq2T96/YMMtw2Dw4QX+F1+g1XSrUCrNyjx7vtFaRDHyB+kobw
dwkpohfkzfTyYpJELzV1r+kMRoyuZ7oIqqccEroMDnnmeApc+BRGbDJqS1Zzk4OA
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     233c8e33 8632ea4e 76d79feb ffb061c6
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
PhoneProxyASA(config)# crypto ca trustpoint CAP-RTP-002_trustpoint
PhoneProxyASA(config-ca-trustpoint)# enrollment terminal
PhoneProxyASA(config-ca-trustpoint)# exit
PhoneProxyASA(config)# crypto ca authenticate CAP-RTP-002_trustpoint
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAyMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEAxCZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhzI85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECnMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NQgZ3YDNoNXg5MmONb8lT86F55EZyVac0XGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbHfM84Duv2Msez+l+SqmqO80kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+sj9+F6KKK2PD0iDwHcRKkcUHb7g
lI++U/5nswjUDIAph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAyL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMlxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaqUtuaSd/m/xzxpcRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH02lPkS/eEQ9sIw6QS7uuHN4y4CJ
NPnRbpFRLw06hnStCZHtGpKEHnY213QOy3h/EWhbnp0MZ+hdr20FujSI6G1+L39l
aRjeD708f2fYoz9wnEpZbtn2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     f7e150ea 5e6e3ac5 615fc696 66415c9f
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
PhoneProxyASA(config)# crypto ca trustpoint Cisco_Manufacturing_CA_trustpoint
PhoneProxyASA(config-ca-trustpoint)# enrollment terminal
PhoneProxyASA(config-ca-trustpoint)# exit
PhoneProxyASA(config)# crypto ca authenticate Cisco_Manufacturing_CA_trustpoint
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAAzANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMDUwNjEwMjIxNjAxWhcNMjkwNTE0MjAyNTQyWjA5MRYwFAYDVQQKEw1DaXNj
byBTeXN0ZW1zMR8wHQYDVQQDExZDaXNjbyBNYW51ZmFjdHVyaW5nIENBMIIBIDAN
BgkqhkiG9w0BAQEFAAOCAQ0AMIIBCAKCAQEAoMX33JaUNRXx9JlOu5tB4X3beRaR
u/NU8kFKlDJiYskj95rnu5t56AcpTjD1rhvFIVZGsPj05o6BuBbMqJuF0kKB23zL
lKkRYRIcXOozIByaFqd925kGauI2r+z4Cv+YZwf0MO6l+IgaqujHPBzO7kj9zVw3
8YaTnj1xdX007ksUqcApewUQ74eeaTEw9Ug2P9irzhXi6FifPmJxBIcmpBViASWq
1d/JyVu4yaEHe75okpOTIKhsvRV100RdRUvsqNpgx9jI1cjtQeH1X1eOUzKTSdXZ
D/g2qgfEMkHFp68dGf/2c5k5WnNnYhM0DR9elXBSZBcG7FNcXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfcWtGwR/dsMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQn88gVHm6aAgkWrSugiWBf
2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1
cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9j
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
AgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy9p
bmRleC5odG1sMF4GA1UdJQRXMFUGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUH
AwUGCCsGAQUFBwMGBggrBgEFBQcDBwYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJ
KwYBBAGCNxUGMA0GCSqGSIb3DQEBBQUAA4IBAQAw8zAtjPLKN0pkmSQpCvKGqkLV
I+ii6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOfTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApcN5JlunGdGTjaubEBEpH6GC/f08
S25l3JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAkPV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd1lZva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIolblPFft6QKoSJFjB6thJksaE5/k3Npf
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     6ea241f5 ac9a1148 cc8b4b43 c7c13025
Do you accept this certificate? [yes/no]: yes

Trustpoint 'Cisco_Manufacturing_CA_trustpoint' is a subordinate CA and holds a non self-signed certificate.
Trustpoint CA certificate accepted.

% Certificate successfully imported
PhoneProxyASA(config)#
```

8. Now that the certificates are on the ASA, we'll need to create the parameters for the CTL file that will be passed down to the phone. In our case, since the tftp server is on the Call Manager (one device serves both roles), we'll create a record-entry of type cucm-tftp (as opposed to just tftp or just cucm). Also note that we use the global (mapped) address for the tftp server here, since this is how the tftp server will look to the phones. The record-entry we add for the CAPF is not required if CAPF certificates are not used:

```
PhoneProxyASA(config)# ctl-file ctl_phoneproxy_file
PhoneProxyASA(config-ctl-file)# record-entry cucm-tftp trustpoint phoneproxy_trustpoint address 14.36.107.95
PhoneProxyASA(config-ctl-file)# record-entry capf trustpoint capf_trustpoint address 14.36.107.95
PhoneProxyASA(config-ctl-file)#
PhoneProxyASA(config-ctl-file)# no shut
Keypair generation process begin. Please wait...

% The fully-qualified domain name will not be included in the certificate
Keypair generation process begin. Please wait...

% The fully-qualified domain name will not be included in the certificate
Keypair generation process begin. Please wait...

% The fully-qualified domain name will not be included in the certificate
INFO: Total CTL File length 4134
INFO: Writing CTL file disk0:/ctl_phoneproxy_file.tlv to flash...
PhoneProxyASA(config-ctl-file)#
```

9. Create the tls-proxy instance. Under this section it is required to specify a trustpoint that was automatically generated by the ASA when the CTL file was created. The trustpoint name will be in the format of *_internal_PP_* + *ctl_file_name*. In this case since the ctl file was *ctl_phoneproxy_file* (see step 8 above) the complete command is **server trust-point _internal_PP_ctl_phoneproxy_file**.

```
PhoneProxyASA(config)# tls-proxy ASA-tls-proxy
PhoneProxyASA(config-tlsp)# server trust-point _internal_PP_ctl_phoneproxy_file
PhoneProxyASA(config-tlsp)# exit
```

10. Create the phone-proxy instance, which outlines the parameters of how the phone-proxy will be configured on the firewall.

The following parameters are configured below:

- The **media-termination address** command ip address should be a unique ip address as defined above
- The **tftp-server address** command ip address should be the internal (real) ip address of the tftp server and the interface should be the interface of the firewall behind which the tftp server resides. Before configuring this parameter, ensure that the static translation for the Call Manager (see step 3) has been created
- The **tls-proxy** command should refer to the name of the tls-proxy instance that was created earlier in step 9
- The **ctl-file** command should refer to the name of the ctl file configured earlier in step 8.
- The **no disable service-settings** specifies that we do not wish the firewall to disable certain settings of the phone

```
PhoneProxyASA(config)# phone-proxy ASA-phone-proxy
PhoneProxyASA(config-phone-proxy)# media-termination address 14.36.107.91
PhoneProxyASA(config-phone-proxy)# tftp-server address 172.18.124.230 interface inside
PhoneProxyASA(config-phone-proxy)# tls-proxy ASA-tls-proxy
PhoneProxyASA(config-phone-proxy)# ctl-file ctl_phoneproxy_file
PhoneProxyASA(config-phone-proxy)# no disable service-settings
PhoneProxyASA(config-phone-proxy)# exit
PhoneProxyASA(config)#
```

11. Define the class-maps that will match the secured traffic. In this case our classes will match the specific TCP ports that the phones will use when making secure sip or skinny connections to the Call Manager. Secure skinny will use TCP port 2443 and secure SIP will use TCP port 5061 by default.

```
PhoneProxyASA(config)# class-map sec_sip
PhoneProxyASA(config-cmap)#  match port tcp eq 5061
PhoneProxyASA(config-cmap)# class-map sec_sccp
PhoneProxyASA(config-cmap)#  match port tcp eq 2443
```

12. Define the policy-map for the phone-proxy functions and apply it to the outside interface:

```
PhoneProxyASA(config-pmap-c)# policy-map voice_policy
PhoneProxyASA(config-pmap)# class sec_sccp
PhoneProxyASA(config-pmap-c)# inspect skinny phone-proxy ASA-phone-proxy
PhoneProxyASA(config-pmap-c)#  class sec_sip
PhoneProxyASA(config-pmap-c)#  inspect sip phone-proxy ASA-phone-proxy
PhoneProxyASA(config-pmap-c)# service-policy voice_policy interface outside
PhoneProxyASA(config)# exit
PhoneProxyASA#
```

13. Using an access-list, permit inbound TFTP traffic to the tftp-server's global IP address. This is the only specific acl entry that needs to exist to allow the phone-proxy to work. The secured streams which terminate on the firewall will be permitted automatically by the firewall.

```
PhoneProxyASA# conf t
PhoneProxyASA(config)# access-list outside_in permit udp any host 14.36.107.95 eq tftp
PhoneProxyASA(config)# access-group outside_in in interface outside
PhoneProxyASA(config)# exit
PhoneProxyASA#
```

At this point the ASA configuration is done. The next step is to go to the phone and ensure that:

- The phone obtains an ip address from the DHCP server on the LAN
- The phone downloads the correct CTL file from the ASA. If the phone previously had a CTL file loaded it should be deleted.
- The phone's tftp server settings are correct (the phone should have a TFTP server ip setting pointing to the global address of the tftp server as defined in the static() command. The TFTP server setting should not point to the media termination address, nor the outside interface ip address of the firewall.

Final completed configuration

The final, complete config for this example is below:

```
ASA Version 8.0(4)
!
terminal width 120
hostname PhoneProxyASA
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 14.36.107.90 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.18.124.241 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
access-list outside_in permit udp any host 14.36.107.95
pager lines 24
logging enable
logging list cucm message 446002
logging buffer-size 1000000
logging monitor debugging
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-524.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 14.36.107.95 172.18.124.230 netmask 255.255.255.255
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto ca trustpoint phoneproxy_trustpoint
 enrollment self
 keypair proxy_key
 crl configure
crypto ca trustpoint capf_trustpoint
 enrollment terminal
 crl configure
crypto ca trustpoint CAP-RTP-001_trustpoint
 enrollment terminal
 crl configure
crypto ca trustpoint CAP-RTP-002_trustpoint
 enrollment terminal
 crl configure
crypto ca trustpoint Cisco_Manufacturing_CA_trustpoint
 enrollment terminal
 crl configure
crypto ca trustpoint _internal_ctl_phoneproxy_file_SAST_0
 enrollment self
 fqdn none
 subject-name cn="_internal_ctl_phoneproxy_file_SAST_0";ou="STG";o="Cisco Inc"
 keypair _internal_ctl_phoneproxy_file_SAST_0
 crl configure
crypto ca trustpoint _internal_ctl_phoneproxy_file_SAST_1
 enrollment self
 fqdn none
 subject-name cn="_internal_ctl_phoneproxy_file_SAST_1";ou="STG";o="Cisco Inc"
 keypair _internal_ctl_phoneproxy_file_SAST_1
 crl configure
crypto ca trustpoint _internal_PP_ctl_phoneproxy_file
 enrollment self
 fqdn none
 subject-name cn="_internal_PP_ctl_phoneproxy_file";ou="STG";o="Cisco Inc"
 keypair _internal_PP_ctl_phoneproxy_file
 crl configure
crypto ca certificate chain phoneproxy_trustpoint
 certificate 0565b348
    308201e1 3082014a a0030201 02020405 65b34830 0d06092a 864886f7 0d010104
    05003035 31333031 06092a86 4886f70d 01090216 2450686f 6e655072 6f787941
    53412e64 65666175 6c742e64 6f6d6169 6e2e696e 76616c69 64301e17 0d303830
    38323630 32303535 375a170d 31383038 32343032 30353537 5a303531 33303106
    092a8648 86f70d01 09021624 50686f6e 6550726f 78794153 412e6465 6661756c
    742e646f 6d61696e 2e696e76 616c6964 30819f30 0d06092a 864886f7 0d010101
    05000381 8d003081 89028181 00bc6a84 b3e0e576 8ffd6d31 184dd17d 24b93112
    cce4105a 37f2aa8a 976eef18 41bd709c d2912432 3be491de ffd96af1 2568f475
    e3ceb134 0a50be49 ced116a7 f1beae19 3a0389ba f95c3ae4 482be283 2870478d
    ddf578ca 9af93be0 20efd4a2 0e1c1cab 8976f1ad a5b3fafd b0bb3c4e 134e33dd
    cdc760cd 980c942a e9dd9f2c 7f020301 0001300d 06092a86 4886f70d 01010405
    00038181 00652195 0df0a0ea b31a825d 387f5592 1986495e 717e03a2 a5db954e
    f063aa64 523728f7 9a3d1985 d6d2028e 9eb0ef66 b2e768df d3b6b3fb fa6deff3
    8c5c3433 46839c5c 7683b186 4cf73843 ba1696f4 40fa02fb 365b1c32 1cc37797
    82870312 4da05a72 09ebef37 ace4e820 b8735c6b cb720f7e 15f2ef85 a2db02d6
    dc1e5ec6 78
  quit
```

Documentation

This configuration example is meant to be interpreted with the aid of the official documentation from the configuration guide located here: Cisco.com ASA 8.0 Configuration guide - Phone Proxy feature Troubleshooting steps for Phone Proxy

Retrieved from "https://supportwiki.cisco.com/ViewWiki/index.php/ASA_Phone_Proxy_sample_configuration"

Category: Cisco ASA 5500 Series Adaptive Security Appliances