Cisco CCA Tool SIP Security methods

The Cisco CCA tool (Cisco Configuration Assistant) provides a graphical interface for configuring the UC500 series devices. Once settings have been established using the tool, the built-in scripting engine configures the IOS based routing components, CUCME (Cisco Unified Call Manager Express) and CUE (Cisco Unity Express – Voicemail) and its use is a quick way to set up the phone system.

The UC500 falls within Cisco's Small Business range of phone systems and components are drawn from Cisco's enterprise voice suite.

When a SIP Trunk is configured on a Cisco IOS device, some very powerful VoIP routing features are enabled. The CCA team have ensured that the configuration script sent to the router results in the end configuration being highly secure. A secure configuration is necessary when connecting the unit (or any other brand PBX system) to an open network such as the Public Internet.

Since the UC500 devices run Cisco IOS, they can be configured from the command line (CLI) as well as CCA. It is therefore important to understand the underlying security techniques used by CCA to avoid these inadvertently being disabled. This has been known to happen, typically when an engineer troubleshoots an inbound calling issue – and the end result can be an increased risk of exposure to a toll fraud attack.

A telephone number associated with a company's main office is known as the 'pilot number'. A telephone number associated with an individual person is known as a DDI or Direct-Dial-Inwards. In the United States, a similar term DID or Direct Inward Dial is used. In either case the expressions deal with inbound numbers and their use can often also refer to the pilot number.

VoIP protocol translator

The UC500 runs a version of Call Manager Express. This software is contained within IOS and runs on the main CPU, controlling the telephones – SIP and SCCP, call routing, call queuing, conferencing and so on. There is also another CPU on an internal hardware module and this module runs a package known as CUE (Cisco Unity Express). CUE is typically used for voice-mail and the Auto attendant. In order for a telephone call to be routed to the CUE module from a SIP trunk, a very powerful function is enabled on the router. This turns the router into a *voice-call* router, and the router now routes phone calls as well as IP packets. Enabled as part of the CUCME/CUE package is SIP->SIP call routing, but also SIP ->H323 ; H323 -> SIP and H323 -> H323. H323 is used as part of the call queuing processes internally. The UC500 is a VoIP protocol translator and the control of how calls are routed is set by the unit's configuration.

Four Security techniques

CCA configures four features which control whether or not calls are processed, and if they're processed how they're routed.

Feature One – Dial-Peer 'permission term'

When a call arrives on a UC500 it is processed by a piece of configuration called an **inbound dial-peer**. Each configured DDI is matched with an inbound dial-peer and after processing is routed to the appropriate destination, eg Hunt group, CUE module, extension, or queue as appropriate.

There is a **special inbound dial-peer**, often numbered by CCA as 'dial-peer 1000 ' which matches ALL incoming calls unless there is a better match. A better match is made if a DDI number has been configured.

```
UC_540#show run | sec dial-peer voice 1000
dial-peer voice 1000 voip
 permission term
 description ** Incoming call from SIP trunk (Generic SIP Trunk Provider)
 session protocol sipv2
 session target sip-server
 incoming called-number .%
 voice-class codec 1
 voice-class sip dtmf-relay force rtp-nte
 dtmf-relay rtp-nte
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
 no vad
```

This special dial-peer has the configuration line "**permission term**". This causes all calls processed by the dial-peer to be dropped. For a SIP call, the response to the sender is a 500 Internal Server Error, which is likely to make a PSTN caller be disconnected, without a meaningful "number busy tone".

The special dial-peer protects the system by the logic "If I don't know about this incoming DDI I'm going to assume it's arriving maliciously and I'm not going to route out via an outbound dial-peer perhaps to the SIP service provider or ISDN Circuit"

Hint. Make sure you configure all your DDI numbers in CCA. CCA will create a series of inbound dial-peers and make sure incoming calls are processed properly. Do not be tempted to remove the 'permission term' from the special inbound dial-peer. Make sure all DDI's are correctly configured.

Feature Two – Voice Source Groups: Calls prefixed with ABCD

A voice source group takes a set of voice sources and treats them in a way defined by some configuration. A source would be identified by its *signaling* IP address. Multiple source groups can be configured on a UC500.

If a voice source group is configured and **if** a call is received from a source which is not contained within ANY voice source group, then the call is rejected. With an incoming SIP call the router responds back to the source with a '500 Internal Server Error'.

The voice source group feature protects the system by the logic "If I don't know about this IP speaker, I'm going to assume it's arriving maliciously and I'm not going to route out via an outbound dial-peer perhaps to the SIP service provider or ISDN Circuit"

CCA defines two source groups, one for internal sources – i.e. CUE module & internal LAN – and one for external sources i.e. the SIP Service Provider.

The voice source group script is processed before the inbound dial-peer is inspected and a number translation tags calls arriving from the CUE module IP, by prefixing calls with the letters ABCD. Another special inbound dial-peer matching calls starting ABCD strips off these letters and lets the call route out as normal. This works around the "permission term" feature which would normally catch calls from CUE if they were destined to go to some random PSTN / extension number.

A voice source is matched to a voice source group by matching the IP address with an IP Access List. CCA typically uses access-list 2 for internal IP address and access-list 3 for external.

```
voice source-group CCA_SIP_SOURCE_GROUP_CUE_CME
 access-list 2
 translation-profile incoming SIP_Incoming !(adds prefix ABCD)
!
voice source-group CCA_SIP_SOURCE_GROUP_EXTERNAL
 access-list 3
dial-peer voice 1003 voip
 description ** Passthrough Inbound Calls for PSTN from CUE **
 translation-profile incoming SIP_Passthrough  !(Strips off ABCD)
 b2bua
 session protocol sipv2
 session target ipv4:10.1.10.1
 incoming called-number ABCDT
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Hint. Incoming call problems from SIP service providers can happen when CCA does not automatically detect the source IP addresses of the service provider. There is a section within the CCA tool for adding in the source IP addresses manually. Do not be tempted to remove the voice-source group security feature, but make sure you have a full list of source IP addresses.

Feature Three – WAN access list

An IP Access List protects the router from incoming IP packets. CCA applies an access list to the WAN interface and configures the list to allow traffic from the SIP Service Provider. Access-list 104 is typically used by CCA.

Hint. Incoming call problems from SIP service providers can happen when CCA does not automatically detect the source IP addresses of the service provider. There is a section within the CCA tool for adding in the source IP addresses manually. Do not be tempted to remove the WAN side access list.

Feature Four – IP Address Trusted List

Recent versions of CUCME have a Toll-fraud feature that works in a similar way to the voice source group feature above. Within the configuration there is a parameter that sets the allowed IP sources for any VoIP communication transiting the system.
Following a software upgrade, the default configuration of this feature leads to calls being rejected with “404 Not Found”. Latest versions of CCA will configure this feature to allow calls to pass, but currently does not configure this feature in a strict way and allows all VoIP sources.

UC_540#show run | sec voice service voip

```
voice service voip
 ip address trusted list
 ipv4 0.0.0.0 0.0.0.0 ! allows all voip sources
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 supplementary-service h450.12
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
```

Hint: A better way of configuring this voice security feature would be to document the allowed voice sources in the configuration as follows in this example

```
voice service voip
 ip address trusted list
 ipv4 10.1.10.0 255.255.255.252 ! Subnet used by CUE
 ipv4 10.1.1.0 255.255.255.0 ! Subnet used internally for voice sources
 ipv4 193.203.210.0 255.255.254.0 ! Subnet for the Service Provider
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 supplementary-service h450.12
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
```